Australia, the utility of force and the society-centric battlespace

MARYANNE KELTON, MICHAEL SULLIVAN, EMILY BIENVENUE AND ZAC ROGERS*

Australia's deployment of military force is motivated by a strong sense of insecurity and belief in alliances with 'great and powerful friends' who share its interests and values.[1] Characterized historically by offshore and expeditionary forward deployments, Australia's use of force reflects not only an insecurity born of limited resources and geographic liminality, but also of a desire to preserve its domestic liberal democratic order and the values informing it, in a regional environment from which threats arise. Australia's method is to meet threats, real and imagined, beyond its borders and bolster national strength through alliances. Since federation in 1901 Australia has almost unquestioningly deployed expeditionary forces in conjunction with British- and then US-led western alliances. This is the case with Australia's most recent military deployments, which were to Afghanistan, Iraq and Syria. However, while the themes of insecurity and reliance on alliances remain, in the emerging cognitive battlespace non-linear[2] changes in adversary strategy and methodology present major challenges to Australia's security strategy.[3]

For Australia, uncertainty in its strategic outlook related to regional and global developments will weigh both on its use of force and on the type of force it can deploy. Shifts in global economic and strategic influence to east Asia over the past decades have been accompanied by escalating regional arms purchases, reducing Australia's reliance on maintaining a 'leading edge' in advanced offensive weapon systems. Sino-US distrust is spiralling, fuelled by events in the South China Sea.

* This article is part of a special issue of *International Affairs* (July 2019) on 'Re-visioning war and the state in the twenty-first century', guest-edited by Tracey German. This article was funded in part by the Defence Science & Technology Group's Strategic Research Investment-Modelling Complex Warfighting grant DST-RA-8381. The insights presented here on the shift to society-centric cognitive warfare are underpinned by the Modelling Complex Human Systems component of the SRI. The views expressed here are the authors' own and in the case of Emily Bienvenue do not represent the official view of the Australian Defence Department. The authors would like to thank Don DeBats, Sian Troath, David Matthews and the anonymous reviewers for their feedback on the research and writing of this article.

[1] Nick Bisley, 'An ally for all the years to come: why Australia is not a conflicted US ally', *Australian Journal of International Affairs* 67: 4, 2013, pp. 403–18; Michael Wesley, 'Dangerous proximity: the collapse of Australia's defences in a contested Asia', *Australian Foreign Affairs*, no. 4, Oct. 2018, pp. 14–34.

[2] In this case in reference to the battlespace we take non-linear to mean qualitative change that does not necessarily progress in a logical or sequenced pattern, e.g. the change from kinetic to cognitive.

[3] See James Lewis, *Cognitive effect and state conflict in cyberspace* (Washington DC: Center for Strategic and International Studies (CSIS), Sept. 2018), https://www.csis.org/analysis/cognitive-effect-and-state-conflict-cyberspace. (Unless otherwise noted at point of citation, all URLs cited in this article were accessible on 21 March 2019.)

International Affairs **95**: 4 (2019) 859–876; DOI: 10.1093/ia/iiz080

Retaliation by both sides hinders broader bilateral relations and raises the risk of escalation,[4] while the consensus in the US policy-making establishment since 2017 is that the 'rules-based liberal order' and US regional primacy are challenged by China's aggressive foreign policy, military buildup and predatory regional economic policies.[5] In addition to perceived state-based threats and widespread competitive nationalisms fuelling changes in regional power dynamics, there are transnational concerns that the return of foreign fighters from the Middle East and west Asia will intensify the likelihood of regional friction.

Burgeoning non-linear changes in the technological, information and cyber-security environment are growing in potency, generating concepts of 'cognitive battlespace' and 'society-centric warfare' that may not be familiar beyond the groups of scholars and specialists working as thinkers and practitioners in the field of cyber warfare. In this article we take the cognitive battlespace to be a unified threat environment where both state and non-state actors 'will be engaged in a continual arms race to influence—and protect from influence—large groups of users online'.[6] In its corollary, the society-centric battlespace, warfare is 'conducted by, within, through and against people and societies'.[7] At present, an emerging suite of complex developments in an era of hyperconnectivity and technological disruption is rapidly reshaping Australia's threat environment. State- and non-state-based adversaries are observable in the cyber domain whose aim is the deliberate long-term disruption of liberal democratic institutions and values. Such disruption has direct socio-political and strategic effects. Such adversaries have global reach, enabled by modern communications infrastructure in a world hyperconnected by large US internet companies and social media platforms. Armed with ample technological capacity and horizontal social peer networks to conduct cyber attacks, these adversaries operate in an unbounded, grey battlespace,[8] wherever networked systems permit access. Classic binary distinctions between peace and war no longer apply.[9] The new challenges are manifest in the disruption of the 2016 Brexit referendum and US presidential election,[10] and, more directly for Australia, in the presence of authoritarian state interference in domestic and regional politics. The frequency and increasing sophistication of

[4] Sam Bateman, 'South China Sea: Paracels in the spotlight', *The Interpreter*, Lowy Institute, 30 May 2018, https://www.lowyinstitute.org/the-interpreter/south-china-sea-paracels-spotlight.

[5] David Shambaugh, 'US–China rivalry in southeast Asia: power shift or competitive coexistence?', *International Security* 42: 4, 2018, pp. 85–127.

[6] Rand Waltzman, 'The weaponization of information', testimony before the Committee on Armed Services, Subcommittee on Cybersecurity, United States Senate, 27 April 2017, p. 7.

[7] Ariel Levite and Jonathon (Yoni) Shimshoni, 'The strategic challenge of society-centric warfare', *Survival* 60: 6, 2018, p. 96.

[8] James Andrew Lewis, *Rethinking cybersecurity: strategy, mass effect, and states*, report of the CSIS Technology Program (Lanham: Rowman & Littlefield, Jan. 2018), p. 16.

[9] Roger C. Molander, Andrew S. Riddile and Peter A. Wilson, *Strategic information warfare: a new face of war* (Santa Monica, CA: RAND, 1996), https://www.rand.org/pubs/monograph_reports/MR661/index2.html; Michele Flournoy and Michael Sulmeyer, 'Battlefield internet: a plan for securing cyberspace', *Foreign Affairs* 97: 5, 2018, pp. 40–46.

[10] Emerson T. Brooking and Peter Singer, 'War goes viral: how social media is being weaponised across the world', *The Atlantic*, Nov. 2016, http://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/; Matthew Hindman and Vlad Barash, *Disinformation, and influence campaigns on Twitter* (Miami: Knight Foundation, Oct. 2018).

asymmetric cyber attacks require strategic-level systemic defence by the Australian government in conjunction with its western allies.

This article argues three central points. First, Australia's use of force historically has been responsive to a strategic culture that valued its liberal democratic origins, while bearing the marks of an anxiety born of insufficient material capability and the country's geographic distance from great and powerful friends. After the end of the Pacific war in 1945, Australia's strategic intent was to ensure the support of the United States via the ANZUS Treaty and other western alliance structures. This will not change.

Second, Australia's use of force in modern irregular warfare in the Middle East and west Asia, and in peacekeeping missions in the south-west Pacific to address an 'arc of instability' from Timor Leste to Fiji, is evidence of this imperative. We examine the deployment of cyber-enabled tactical intelligence, surveillance and reconnaissance and electronic warfare (EW) capabilities to Iraq. However, the protracted nature of these conflicts, and the catalytic consequences of the Syrian civil war, have raised sombre 'means and ends' dilemmas for Australian war-making, as the use of force, while still driven by insecurity, has been decoupled from the strategic objective of securing Australia. The utility of Australia's force equations also changed as the adversary and its methodology changed. A reformulated 'force of politics rather than the politics of force',[11] evident first in Al-Qaeda, has been apparent in the use of the internet and social media platforms by the Islamic State in Iraq and Syria (ISIS). In 2016, Russia's 'active measures' in the US presidential elections were designed to achieve broad socio-political impact on international stability and the stability of western democracies,[12] while China's interference was felt in Australia and New Zealand.

Third, the evolving cognitive and society-centric battlespaces present considerable challenges to Australia's traditional strategic rationale for the use of force, including threat perceptions, force structure and posture agreements, and resourcing. Capability and innovation challenges in a technologically changing strategic landscape are driving Australia to closer connectivity with the United States. A troublesome question remains as to how offensive and defensive force is constructed and applied in a new unified threat environment only recently being recognized in Australia.

Shifting liminality

Australia's military history, and the strategic culture upon which it is based, are illustrative of a deeply rooted insecurity born of structural and cultural interpretations of Australian strategic vulnerability. Historically, Australia lacked capacity to defend its settlement, society and western liberal democratic values.

[11] Clint Watts, *Messing with the enemy: surviving in a social media world of hackers, terrorists, Russians, and fake news* (New York: HarperCollins, 2018), p. 131.

[12] The hybrid threat toolkit is explained by Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee and Madeline McCue, *Addressing hybrid threats* (Stockholm: Centre for Asymmetric Threat Studies, European Centre of Excellence for Countering Hybrid Threats, Swedish Defence University, 2018).

It continues to be conscious of a limited capacity to contribute to the defence of the rules-based international order on which its trade-dependent maritime status and value-systems rely. The insecurity of its small population, coastally congregated around a large land mass, has been understood through a British settler/colonial lens. The sense of insecurity was exacerbated by the 'tyranny' of distance both continentally and globally, and the demands of its island geography. Though Australian civil society since federation in 1901 is demonstrably peaceful, Australian defence forces have participated in all subsequent expeditionary operations of significance, initially with Britain and then with the United States. Australia has aligned itself with these great and powerful friends on the basis of their western democratic values and their capacity to provide a secure economic environment.[13]

In military practice after the release of the influential Dibb Report in March 1986 a strategic culture determined predominantly by Anglo-American influence and desire to operate within larger constructs[14] was manifested through a 'self-reliance within alliance' framework.[15] Nonetheless, Australia's strategic culture and practice worked to keep the country connected to Britain and the Commonwealth, and then to the United States and the 'Five Eyes' alliance through the ANZUS and UKUSA treaties, and governmental and military networks and operations.[16] In the 1980s, Australia's moves towards greater self-reliance and regional cooperation through closer defence ties and joint military exercises remained embedded within the US alliance, and governed by the implicit understanding that Australia was covered by the (unstated) provisions of a US extended deterrence policy.[17] Stark realization of the degree of Australia's reliance on the US alliance became evident with the US contribution of essential diplomatic and logistical support during the 1999 East Timor independence crisis, without which Australia would have been unable to deploy to the zone of conflict. Since the early 2000s, however, Australia's historical fear of its liminality has been mitigated for defence policy-makers by the shift of economic growth and dynamism to east Asia, though China's rising power poses a new raft of strategic challenges. As noted in each of Australia's three most recent defence white papers (2009, 2013 and 2016), China's increasing assertiveness is identified as both a strategic challenge to regional security and an implicit determining factor in arguments for increased defence spending and future patterns of military procurement.

[13] David Kilcullen, 'Australian statecraft: the challenge of aligning policy with strategic culture', *Security Challenges* 3: 4, 2007, pp. 45–65 at p. 51.

[14] Graeme Cheeseman, 'Australia: the white experience of fear and dependence', in Ken Booth and Russell Trood, eds, *Strategic cultures in the Asia–Pacific region* (Basingstoke: Macmillan, 1999), pp. 273–98; Richard Higgott and Kim Richard Nossal, 'Australia and the search for a security community in the 1990s', in Emanuel Adler and David Barnett, eds, *Security communities* (Cambridge: Cambridge University Press, 1998), pp. 265–88.

[15] Department of Defence, *The Defence of Australia 1987* (Canberra, 1987), http://www.defence.gov.au/Publications/wpaper1987.pdf.

[16] The Five Eyes alliance refers to intelligence-gathering and sharing arrangements between the US, Britain, Australia, Canada and New Zealand. See Andrew O'Neil, 'Australia and the "Five Eyes" intelligence network: the perils of an asymmetric alliance', *Australian Journal of International Affairs* 71: 5, July 2017, pp. 529–43.

[17] Stephan Frühling, 'The fuzzy limits of self-reliance: US extended deterrence and Australian strategic policy', *Australian Journal of International Affairs* 67: 1, 2013, pp. 18–34.

Recent forward and allied deployments in an evolving battlefield

Australia's missions from the early 2000s onwards reveal attention to longstanding themes in Australian forward deployment. Australia's values and interests, outlined in three foreign policy white papers (1997, 2003 and 2017), were a constant in strategic support for the rules-based liberal international order. Nonetheless, the battlefield missions undertaken by the Australian Defence Force (ADF) in the early 2000s as a consequence of alliance contingencies arguably forced the decoupling of values from the utility of force calculus. Australia's commitment to the use of force in forward deployments to Afghanistan and Iraq was highly contingent on US policy-making and operational engagement with the 'coalition of the willing'. Yet 'defence of international order' arguments justifying armed intervention could not be sustained easily by either the United States or Australia, given their inability to articulate achievable political outcomes in Afghanistan amounting to 'victory'. Thus an effective and successful in-country war-fighting strategy, in both Iraq and Afghanistan, was reduced to the achievement of tactical gains at the risk of alienating local communities.[18] Despite the broader alliance pressures compelling Australia to engage in forward defence with the United States, its risk mitigation strategy was politically expansive but operationally constrained.

The forward deployment of military force in conjunction with the United States has bipartisan support in Australia in party-political terms, though differences appeared as the Iraq and Afghan deployments dragged on. In 2010 Labor Prime Minister Julia Gillard echoed the initial rationale of an earlier coalition government in asserting that Australia's two vital national interests determining the ongoing Afghan mission were (a) the elimination of a safe haven for terrorists and (b) the fulfilment of Australia's alliance commitments.[19] Through the extended duration of both wars and a constant awareness of their flawed utility for national security, Australia sustained the deployment of military force within a variety of iterations of the US mission. Once the initial phase of the Afghanistan war (September 2001 to December 2002) was complete, Australia's three squadrons of special forces withdrew, only for the ADF to redeploy a further special forces task group in 2005 as the United States reignited offensive operations. Australia also provided air support via F/A-18 Hornets out of Diego Garcia in the Indian Ocean and B-707 air-to-air refuellers out of Kyrgyzstan. These assets were deployed together with four reconstruction groups to assist the Dutch Provincial Reconstruction Task Force in Uruzgan province. Eventually, under alliance pressures, Australia reluctantly assumed command of that group after the Dutch withdrew in August 2010. By 2012 Australia's deployment numbered

[18] Albert Palazzo, 'Strategy and securitisation: conflict or complement in Australian operations in Afghanistan', *Australian Army Journal* 14: 1, Autumn 2018, pp. 41–55 at pp. 43, 50.

[19] Julia Gillard, 'No safe haven', prime ministerial statement to House of Representatives, Canberra, 19 Oct. 2010, https://www.theaustralian.com.au/national-affairs/defence/julia-gillards-speech-to-parliament-on-australias-deployment-to-afghanistan/news-story/a34f7551f3eab7e848e6489584aca4ba; John Howard, 'Application of ANZUS Treaty to terrorist attacks on the United States', prime ministerial statement to House of Representatives, Canberra, 14 Sept. 2001, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22media/pressrel/YFY46%22.

1,500 personnel in Afghanistan and 800 across the wider Middle East. Despite the diminished expectations for a reconstructed Afghanistan, and conceding that the Taliban controlled large swathes of the country, the Australian commitment, as part of the US-led International Security Assistance Force (ISAF) mission, held fast to the aim of preventing Afghanistan being used as a safe haven for terrorism. As ISAF prepared to depart in 2013, a minimalist position of denying a safe haven for international terrorists may have been achieved; but the evolving objective of nation-building was not realized and, as was eventually acknowledged, the ADF was ill-equipped to achieve it.[20]

The effectiveness of the western states' traditional application of force was jeopardized in Afghanistan by a complex array of political, social and military challenges. The use of military force in Afghanistan to defeat global terrorism was ineffective because of the ineffectual nature of the Karzai government and pervasive elite corruption, as illustrated by the collapse in September 2010 of the Kabul Bank as a result of fraud; the absence of legitimate and functional governance structures throughout the provinces; the dependence upon the international community that has also provided cover for government failures; dysfunctional relationships between foreign and local forces; and the 'insurgent sanctuaries' ranging across the Durand Line which have meant that ISAF and Afghan National Security Forces (ANSF) are unable to pursue insurgents into Pakistan.[21] Personal accounts of a growing number of soldiers expressed a sense of futility while on duty. Concern among the Australian public also grew as the conflict dragged on, with ADF casualties reaching 41 deaths, 261 major injuries and an unspecified number of service personnel affected by post-traumatic stress disorder. Not only was the battlefield changing, but the strategic war of ideas to achieve victory could not be prosecuted through the tactical deployment of military force.

Cyberspace: tightening alliance contingencies

For Australia, the changes from the battlefield to the cyber-enabled battlespace became more evident in the complex and messy wars in Iraq and Syria. As Australia gained valuable operational experience in Iraq, and as operations connectivity and interoperability with the United States matured in the 2010s,[22] the nature and utility of military force were reshaped by a widening and deepening evolution of cyber threats. Yet development of an alliance strategy on the nature of these new threats, and development and deployment of new defensive and offensive capabilities in the emerging battle domains, lagged behind. Australia's calculus in committing to the use of military force persisted with a focus on traditional alliance

[20] Peter Leahy, 'Time running out to fix strategy', *The Australian*, 19 July 2011; Simon Cullen, 'General criticises Australia's Afghan "experiment"', ABC News, 24 Sept. 2012, http://www.abc.net.au/news/2012-09-24/former-top-commander-criticises-afghan-war/4277240.

[21] Raspal Khosa, *Towards transition: prospects for progress in Afghanistan in 2011*, Policy Analysis no. 81 (Canberra: Australian Strategic Policy Institute (ASPI), 1 June 2011), pp. 4–5.

[22] Leo Davies, 'A fifth-generation air force: alliance structures and networked capabilities from an Australian perspective', presentation to CSIS, 11 May 2017, https://www.csis.org/events/fifth-generation-air-force-alliance-structures-and-networked-capabilities-australian.

tactics, operations and capabilities. Alliance deployments in the Middle East and western Asia allowed access to and integration with the evolving cyber-enabled, networked battlespace being deployed by the United States, including the use of EW and navigation warfare in the denial, degradation, disruption and destruction of command, control and communications networks, weapons and integrated air defence systems. Allies were also protected through identification of ambush ploys and jamming of remotely controlled improvised explosive devices. EW had also come to the fore in 2007 when Syria's air defence systems were disabled, allowing Israeli air force F-15Is and F-16Is to destroy a nuclear facility under construction just outside Deir Ezzor in the east of Syria.

Australia's role in the US normalization of networked cyber warfare eventually extended beyond the confines of the battlespace. While the US General Petraeus-led 'surge' in Iraq in 2007–2008 was ineffective because of the absence of a long-term vision for post-conflict reconstruction of state and society,[23] its operational and tactical victories were enabled by implementing the National Security Agency's data-mining and processing system in 2007. This permitted the United States to sweep insurgent electronic communications and networks, collecting huge amounts of data via human and signals intelligence, and airborne and space sources, which were then used in an unprecedented manner in real-time operations. In 2010 this system was implemented in Afghanistan, using civilian data to forecast prospective conflict points. In subsequent iterations the data system was integral to a strategy of 'virtual isolation' of ISIS.[24] Major infrastructure developments at the Australia–US Joint Defence Facility in Pine Gap were instrumental[25] in the successful US digitalization and exploitation of its offensive cyber-warfare capabilities. Australia expanded its crucial intelligence relationship with the US National Reconnaissance Office, from monitoring satellite systems and ballistic missile launches to becoming a key provider of tactical and operational battlefield intelligence in Asia and the Middle East.[26] In addition, it facilitated burgeoning cooperation in space, which emerged as a defined battlespace because of developments in anti-satellite weapons systems. Though this prompted Australia to consider joint investments with commercial partners in indigenous space-based sensor systems, in the event a Space Situational Awareness Partnership with the United States came into effect in 2010, reinforcing the alliance. Australia was given access to the US Wideband Global Satcom system, extending the capacity of the alliance in orbital surveillance and intelligence, with Australia gaining 'full knowl-

[23] Steven Simon, 'The price of the surge: how US strategy is hastening Iraq's demise', *Foreign Affairs* 87: 3, May–June 2008, pp. 57–76.

[24] Statement of Gen. Joseph F. Dunford, Committee on Armed Services, US Senate Hearing to receive testimony on counter-ISIL (Islamic State of Iraq and the Levant) operations and Middle East strategy, 27 April 2016, p. 39.

[25] Desmond Ball, Bill Robinson and Richard Tanter, 'Management of operations at Pine Gap', NAPSNet Special Report, 24 Nov. 2015, http://nautilus.org/wp-content/uploads/2015/11/PG-Managing-Operations-18-November-2015.v2.pdf.

[26] Richard Tanter, 'The "joint facilities" revisited—Desmond Ball, democratic debate on security, and the human interest', NAPSNet Special Report, 11 Dec. 2012, pp. 26-32, https://nautilus.org/napsnet/napsnet-special-reports/the-joint-facilities-revisited-desmond-ball-democratic-debate-on-security-and-the-human-interest/.

edge' of activities 'in, through or from' its territory.[27] Under the agreement, work was undertaken on a jointly operated C band surveillance radar designed to increase knowledge of foreign satellite operations.

Facilities at the Australian Defence Satellite Communication Station and Harold E. Holt Station in Exmouth were upgraded, along with the relocation of an optical surveillance telescope from the US Defense Advanced Research Projects Agency to provide more extensive surveillance and communications across Asia and the Middle East. In 2014 the United States, United Kingdom and Australia extended space cooperation to facilitate massive increases in data collection and real-time processing, with access extending potentially into Five Eyes collaboration. It is likely that these arrangements will also make military and intelligence contributions to the new inter-agency National Space Defense Center in Colorado Springs, which became operational in January 2018. Though Australia is aware that technological advances in satellite-to-satellite communications, which centre on quantum systems, optical communications and satellite-based laser systems, may in the longer term downgrade the facilities at Pine Gap,[28] the importance of the latter as a primary ground-based detection and communication facility may be enhanced by a potential adversary's rapid development of asymmetric cyber-warfare and anti-satellite weapons systems. Institutional alliance integration continues to evolve, but America's far greater capacity to innovate and devote resources to the development of its cyber-warfare strategies and networks means that Australia's reliance on the US alliance is increasing rather than decreasing as deployments to Afghanistan, Iraq and Syria wind down.[29]

As Australia's conceptualization of 'self-reliance within alliance' tilted towards the 'alliance', its continuing asymmetrical reliance on the United States was noted by Ball and colleagues in 2016:

> Pine Gap remains a United States facility, which was both established and then greatly expanded to satisfy US intelligence and warfighting interests. High policy direction, command arrangements, priorities of operational tasking, and the globe-spanning socio-technical space-based systems of which Pine Gap is an integral part all confirm that Pine Gap is a US facility in the operation of which Australia participates closely.[30]

Peter Jennings, Executive Director of the Australian Strategic Policy Institute (ASPI), also observed that 'the design of our Navy and Air Force hinges on the alliance getting even closer. If alliance cooperation ended we might as well close some of our intelligence agencies and get used to dealing with the region substantially blind-sided'.[31] Yet after 2013, Australia's immediate Indo-Pacific security

[27] Jeffrey Richelson, *The US intelligence community* (Boulder, CO: Routledge, 2016), p. 379.
[28] David Schaefer, 'Intelligence cooperation and new trends in space technology: do the ties still bind?', *Australian Journal of International Affairs* 72: 4, pp. 31–48 at pp. 36–7.
[29] Kim Beazley, 'The alliance—dependence grows as our options narrow', *The Strategist*, ASPI, 1 May 2018, https://www.aspistrategist.org.au/alliance-dependence-grows-options-narrow/.
[30] Desmond Ball, Bill Robinson and Richard Tanter, *Australian participation in the Pine Gap enterprise*, Nautilus Peace and Security (NAPSNet) special report, 9 June 2016, http://nautilus.org/napsnet/napsnet-special-reports/australias-participation-in-the-pine-gap-enterprise.
[31] Peter Jennings, *Trump means we need a Plan B for defence* (Canberra: ASPI, 21 July 2018), https://www.aspi.org.au/opinion/trump-means-we-need-plan-b-defence.

environment was increasingly uncertain, given the strategic implications of China's building and militarizing a series of bases on artificial islands in the Spratly archipelago,[32] and regional instability arising from the return of foreign fighters from the Middle East, as evidenced by the 2017 siege of Marawi by supporters of Islamic State in the Philippines.[33] The alliance relationship with the United States thus became more valuable as Australia–US interoperability continued to evolve. In 2018, cooperation involved developing plans to respond to escalating Indo-Pacific missile threats, and to advance joint research and development in cyberspace technologies, hypersonics and quantum computing.[34]

A more pervasive socio-cognitive battlespace

Australia has encountered radical and complex changes in the strategic trajectory and methodology of non-state adversaries in the cyber battlespace. Beginning in the Middle East and extending globally, these changes eventually resulted in what may be called society-centric, cognitive warfare. The ideas informing cognitive and society-centric warfare predate the digital age. As Galeotti reminds us, George Kennan wrote of 'political war', where 'subversion' to control information through 'white propaganda' and 'black psychological warfare' is not the prelude to war, but war itself.[35] It is just that the 'weaponization' of social media, seen as a tool of cyber warfare used on a grand scale in the 2016 US elections, seems to confirm the good and bad roles of existing technologies in delivering on the promises of cognitive and society-centric warfare identified by earlier generations, with the expectation that emerging technologies, such as artificial intelligence and quantum computing, will take cyber-enabled warfare to new levels of social opportunity and military threat. Ariel Levite and Yoni Shimshoni also remind us that in many traditions of strategic thinking the importance of 'society' is stressed, but is then often overlooked when strategy is reduced to the deployment of military force. They point out that:

> While the social dimension has long been deeply ingrained in warfare and strategy, its centrality to twenty-first-century conflict has become extreme. Virtually all the actors now challenging the West—large and small, state and non-state, from al-Qaeda and Hamas to China and Russia—have adopted multifaceted strategies with society at their core. Indeed, these could be called society-centric strategies.[36]

They argue that warfare is always a struggle between 'societies', and that in the era

[32] Australian Government, *2017 foreign policy white paper: opportunity security strength* (Canberra, 2017), https://www.fpwhitepaper.gov.au/foreign-policy-white-paper.

[33] Bjørn Grønning argues the increased value of the US alliance from the Japanese perspective: 'Operational and industrial military integration: extending the frontiers of the Japan–US alliance', *International Affairs* 94: 4, July 2018, pp. 755–72 at p. 772.

[34] Department of Defence, *Joint statement, Australia–US ministerial consultations ('AUSMIN') 2018*, 24 July 2018, https://www.minister.defence.gov.au/minister/marise-payne/statements/joint-statement-australia-us-ministerial-consultations-ausmin-2018.

[35] Mark Galeotti, 'I'm sorry to have created the "Gerasimov doctrine"', *Foreign Policy* online, 5 March 2018, https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/.

[36] Levite and Shimshoni, 'The strategic challenge of society-centric warfare', p. 92.

of cognitive warfare this means that defence forces must work out how to define their 'mission statement' in terms of 'engaging the social dimension'. Conversely, the challenge for social institutions is to accept a greater role for the defence forces in cyber security.

While existing and future adversaries in the cyber domain will attack largely from offshore, their threats cannot be met by forward deployment of force or expeditionary force as part of an alliance campaign, at least as understood traditionally. The threats are 'cognitive' and 'society-centric' in that they involve the weaponization of information, especially social media. Attacks are launched from outside into the very heart of the institutions and values that Australia has had a strong sense of insecurity about since Federation. Though insecurity and alliance remain constants, the threat of society-centric warfare turns Australian strategic thinking on its head. The understanding of the utility of force—to defend Australia by fighting as far away from Australia as possible, or by controlling the northern 'air-sea gap' approaches to Australia—breaks down because in cyberwarfare national borders are breached without the use of kinetic force. The aim of the breach is to gain access to and manipulate information; either to steal valuable data or to insert false data and let it go viral. The ultimate goal is to infect the network with algorithms so that it creates and distributes its own false information while seemingly acting normally. The challenge for the massive national security bureaucracy is whether it is agile enough to respond strategically to the idea of cognitive warfare. The challenge for legislators and civil society is whether traditional legal constraints on the role of the military in domestic civilian affairs help or hinder national cyber security, when the threat is society-centric.

These more dangerous, sustained and pervasive challenges evolved rapidly in a non-linear manner across a new global threat environment after 9/11. Al-Qaeda used the internet to great effect in networking its ideology, radicalizing recruits, and coordinating and financing operations from the isolated reaches of Tora Bora in eastern Afghanistan's Spin Ghar region and the Federally Administered Tribal Areas of Pakistan. In the Horn of Africa, Al-Shabaab perfected the use of YouTube, Facebook and Twitter to network with vulnerable young prospective recruits in the West. With the emergence of ISIS in Iraq and Syria, Australia's defence forces encountered an enemy mobilized and enabled through social media.[37] Moreover, together with the hacker group known as the Syrian Electronic Army, which supported the Syrian President Bashar al-Assad, from 2011 the adversary targeted western media outlets, relocating the shifting weight of the battlespace to cafés and lounge rooms across the globe. No matter what operational and tactical battles were won in theatre, a decisive strategic victory became more elusive as adversaries targeted civilians, not militaries, especially in liberal democracies. If, as Palazzo argues, 'war is won and lost in the mind of the people',[38] then attacking the cognitive battlespace is a compelling logic for any belligerent in a fluid, asymmetric

[37] J. M. Berger, Testimony for hearing before the Committee on Homeland Security and Governmental Affairs, US Senate Hearing 114-438, Washington DC, 7 May 2015, 'Jihad 2.0: social media in the next evolution of terrorist recruitment', https://www.gpo.gov/fdsys/pkg/CHRG-114shrg95653/html/CHRG-114shrg95653.htm.

[38] Palazzo, 'Strategy and securitisation', p. 45.

conflict. The ADF was compelled to begin thinking about defence through attack and the offensive potential of cognitive warfare.

As Australia's post-9/11 operating environment against non-state adversaries evolved into the territory of cognitive warfare, it became evident that state-based actors were using the hyperconnectivity of the new social media in attempts to disrupt and delegitimize western liberal democratic values for strategic effect.[39] Globally, the contours of the cognitive battlespace were characterized increasingly by unbounded competition manifested below the threshold of kinetic warfare and with no clearly demarcated front line. To comprehend the nature of this threat posed to liberal democracies such as Australia and its allies, it is helpful first to remind ourselves how international order is established and maintained. As Andrew Phillips has stated:

> In stable orders these (moral) values generally secure wide assent among the order's constituent polities . . . International orders are sustained through a combination of authoritative institutions, which attract agents' compliance through their concordance with shared standards of legitimacy, and coercive institutions, which compel agents' compliance through the application of authorised practices of organised violence.[40]

The new and enveloping challenge is aimed directly at degrading the legitimacy of, and compliance with, constituent polities and authoritative institutions. What makes the liberal international order especially vulnerable to an adversary's quest to weaken the polis and undermine the legitimacy of institutions is that the challenge resonates with *both* Ikenberry's 'Polanyi' crisis, whereby global capitalism outstrips its political foundations, and the 'E. H. Carr' crisis, whereby Great Power strategic competition and anarchy resurface.[41] What links the two 'crises' is the adversary's attacks using social media on liberal democracy's domestic values and institutions, at a time when 'multilateral overreach' is precipitating the rise of populism, illiberalism and economic nationalism. These digitally enabled pressures on the divisible seams in the socio-economic and political fabric exacerbate the existing vulnerabilities particularly around inequality.[42] Dissonance between governing institutions and the body politic creates ripple effects that fracture the fiduciary relationship between citizens and government.[43] Social intelligence derived from advances in digital technology, artificial intelligence and machine learning, and the neurological and algorithmic sciences are deployed to exploit vulnerabilities in social networks and effect disruptive political, social and economic change.[44] Operationalized cognitive attacks 'inject fear, anger, anxiety,

[39] Chris Demchak, 'Uncivil and post-western cyber Westphalia: changing interstate power relations of the cybered age', *Cyber Defense Review* 1: 1, 2016, pp. 49–74.

[40] Andrew Phillips, *War, religion and empire: the transformation of international orders* (Cambridge: Cambridge University Press, 2011), pp. 5–6.

[41] G. John Ikenberry, 'The end of liberal international order?', *International Affairs* 94: 1, 2018, pp. 7–23 at p. 10.

[42] Jeff Colgan and Robert Keohane, 'The liberal order is rigged; fix it now or watch it wither', *Foreign Affairs* 96: 3, 2017, pp. 36–44.

[43] *War and the human brain, with Dr James Giordano*, Modern War Institute podcast, interview with John Amble, 24 July 2018, https://mwi.usma.edu/mwi-podcast-war-human-brain-dr-james-giordano/.

[44] Laura Donohue, 'The dawn of social intelligence (SOCINT)', *Drake Law Review* 63, 2015, https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2540&context=facpub.

uncertainty, and doubt into the adversary's decision-making processes', and are enabled to do so through the high-connectivity, low-latency, disintermediated, inexpensive and deterritorialized utility of the internet space.[45] The 'trust-based' attacks on Sony and the Democratic National Convention in the United States in 2016 are illustrations of this cognitive effect. It is in the light of these developments that James Lewis argues that the West has 'misperceived cyber risk'.[46] While the United States and its allies pursued technological dominance as an end in itself, they failed to comprehend the target of Russia's 'strategy of technology', or 'hybrid war', which is to produce a cognitive effect by undermining the western rules-based order.[47] Given Russia's continuing cyber- and social-media based political influence campaigns, national security has to be understood in a 'world of audiences not defined by the borders of our country'. According to Clint Watts, the Russian agenda is to pursue an international, anti-democratic destabilization strategy and sponsor an anti-globalist nationalist agenda, particularly on immigration and refugees, to which Australia is susceptible.[48] The goals in the society-centric cognitive battlespace, it seems, are: first, to arouse doubt and confusion, so as to reinforce an adversary's own domestic propaganda campaigns against the utility of the 'western model'; and second, to diminish the moral attractiveness and viability of the western rules-based liberal international order in the Indo-Pacific during a time of Great Power transition.

This change in how national security and the utility of military force must be calculated is also observed in the growing awareness among intelligence agencies, media and governing elites in liberal democracies of foreign government interference beyond traditional political influence campaigns. Foreign and defence policy-makers and officials are constantly defending the 'rules-based liberal international order' and US primacy in the Pacific as the security guarantees of regional stability and prosperity.[49] They are also expressing growing concern about the nature and extent of the influence of China's ruling Communist Party, including its intentions and capacity to leverage an expanding regional presence. Australia is targeted because of its sense of strategic and economic vulnerability, and its reliance on the US alliance at a time of misgivings about President Trump's foreign policy, and because China is Australia's most significant trading partner by some measure. The Communist Party's intention is to cast China's regional activities in a positive light and negate criticism, while working with agents of influence to accommodate Chinese interests in Australia and the region under the guise of 'win–win' outcomes. Australia's 2017 foreign policy white paper states that 'the Government

[45] Herbert Lin and Jaclyn Kerr, *On cyber-enabled information/influence warfare and manipulation*, working paper (Stanford, CA: Center for International Security and Cooperation, 13 Aug. 2017), pp. 6–7, https://cisac.fsi.stanford.edu/publication/cyber-enabled-informationinfluence-warfare-and-manipulation.

[46] Lewis, *Rethinking cybersecurity*, pp. 10–15.

[47] James Wirtz, 'Cyber war and strategic culture: the Russian integration of cyber power into grand strategy', in Kenneth Geers, ed., *Cyber war in perspective: Russian aggression against Ukraine* (Tallinn: NATO Publications, 2015).

[48] Clint Watts, panellist for Eric Rosenbach, *The digital threat to democracy*, Kennedy School Institute of Politics, Harvard University, 11 Sept. 2017, https://www.youtube.com/watch?v=zgiH8Y8chWE.

[49] Department of Defence, *2016 defence white paper* (Canberra, 2016).

is concerned about growing attempts by foreign governments or their proxies to exert inappropriate influence on and to undermine Australia's sovereign institutions and decision-making'.[50] Moreover, Duncan Lewis, Director-General of Security at the Australian Security Intelligence Organisation (ASIO), advises that, in ASIO's assessment, 'the current scale of foreign intelligence activity against Australian interest is unprecedented';[51] but public awareness about this threat to national security is disturbingly limited.[52] Unrestrained by longstanding, arbitrary distinctions in the West between civilian/military and public/private components of a state's interest and pursuit of power, China talks instead of civilian–military 'fusion'. The Communist Party declares openly that its informationalization strategy is integral to the exercise of comprehensive national power.[53] Regarding the pursuit of influence to sow seeds of doubt between citizens and the government, and to fashion pro-China attitudes, John Garnaut concludes that China's 'international influence system is a complex, subtle and deeply institutionalised set of inducements and threats designed to shape the way outsiders talk, think and behave'.[54] Though the focus of strategic analysis and assessment is China's terraformation in the South China Sea and its demonstration of its rapidly expanding and lethal power projection capabilities, King and colleagues argue that 'considerably more effort' is needed urgently 'on the Chinese Internet and its information environment, which is a contested virtual space, one that may well be more important than many contested physical spaces'.[55] As awareness grows of China's state-directed political influence activities, the Australian government harbours increasing concerns for domestic and regional democratic processes and security.

Configuring Australia's defence force: cyber *and* cognitive?

Though preoccupation with counterterrorism consumed much of Australian strategic thinking after 9/11, realization of the need to understand the state-based cyber and networked characteristics of force grew slowly in the country's threat assessments. Cyber intrusion and espionage were on the rise.[56] Infiltration of the Bureau of Meteorology (BOM) by Chinese hackers in 2015 demonstrated the degree to which government departments are vulnerable.[57] Its importance as a

[50] Australian Government, *2017 foreign policy white paper*, p. 75.

[51] Duncan Lewis, Testimony before Senate Legal and Constitutional Affairs Legislation Committee, Estimates, Canberra, Thursday 24 May 2018, p. 149.

[52] David Martin Jones, 'Intelligence and the management of national security: the post 9/11 evolution of an Australian national security community', *Intelligence and National Security* 33: 1, 2018, pp. 1–20 at p. 14.

[53] Information Office of the State Council of the People's Republic of China, *China's national defense in 2004* (Beijing, Dec. 2004), http://www.china.org.cn/e-white/20041227/.

[54] John Garnaut, 'The rest of the world is watching how we counter Beijing's campaign of influence', *The Monthly*, Aug. 2018.

[55] Gary King, Jennifer Pan and Margaret Roberts, 'How the Chinese government fabricates social media posts for strategic distraction, not engaged argument', *American Political Science Review* 111: 3, 2017, pp. 484–501 at p. 497.

[56] Australian Cyber Security Centre, *ACSC 2016 Threat Report*, https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf.

[57] Chris Uhlmann, 'China blamed for "massive" cyber attack on Bureau of Meteorology computer', ABC News, 2 Dec. 2016, http://www.abc.net.au/news/2015-12-02/china-blamed-for-cyber-attack-on-bureau-of-meteorology/6993278.

target is that the BOM's systems reach across government departments, including links into defence, and it plays an important role in satellite coordination. Its vulnerability offered, in hindsight, an obvious entry point for an adversarial actor with knowledge of how Australia's cyber networks interconnect and are secured. Worryingly, in 2016 the Australian National Audit Office advised that key government agencies, including the Department of Immigration and Border Protection (which became part of the Department of Home Affairs 'super-ministry' in September 2017) and the Australian Tax Office, were neither compliant with cyber-mitigation strategies nor cyber resilient.[58] In February 2019 it was revealed that the federal parliament's computer systems had been hacked by a state-based actor, as had the networks of the three major political parties, the Australian Labor Party, the Liberal Party and the National Party.

In recognition of the need for enhanced cyber security, Australia's nascent cyber forces were reconfigured in 2016. This proved to be a turning-point. Given little choice but to acknowledge an increasing threat to national security, the Australian government enacted structural and policy changes, establishing the Australian Cyber Security Centre, issuing the first Cyber Security Strategy and Threat Report (2016) and creating new senior cyber-security positions, while supporting national, holistic cyber resilience across government, corporate and community sectors.[59] To enhance joint network warfare capabilities, the Information Warfare Division was established in July 2017, comprising an Information Warfare Capability, a C4I[60] and Battle Management Capability, a Capability Support Directorate and a Joint Cyber Unit.

The acquisition of an offensive cyber capability was a watershed in Australia's generation of and commitment to new offensive force platforms and capabilities, albeit in a battlespace that was much less visible and obvious to outside observers than those of traditional engagements. Following the US lead, Prime Minister Turnbull stated in April 2016 that Australia had deployed an offensive cyber capability housed in the Australian Signals Directorate (ASD).[61] The Australian government declared that it would use this capability to deter and respond to serious cyber attacks on any local network launched by state-based adversaries; support military operations, including coalition operations against ISIS in Iraq and Syria; and counter offshore cybercriminals. Given the ASD's role in intelligence-gathering, these operations will integrate big data, artificial intelligence and machine learning with cyber operations, thus establishing a mission-critical element of national security and ensuring success in a conflict.[62]

Digital connectivity among networked allies in the new battlespace is crucial to Australia's response to the evolving challenges to national and regional security. The formal statement of the prime minister and cabinet on cyber strategy in 2016

[58] Australian National Audit Office, *Cybersecurity follow-up audit*, 15 March 2017, https://www.anao.gov.au/work/performance-audit/cybersecurity-follow-audit.
[59] Australian Signals Directorate, *Australian Cyber Security Centre*, https://www.acsc.gov.au.
[60] Command, control, communications, computers and intelligence.
[61] Malcolm Turnbull, 'Launch of Australia's Cyber Security Strategy', 21 April 2016, https://www.malcolmturnbull.com.au/media/launch-of-australias-cyber-security-strategy.
[62] Prime Minister and Cabinet, 'Prime Minister launches Cyber Security Strategy', media release, 22 April 2016.

promoted stronger domestic and regional defence with partners, while defending the value of a 'strong, free, and open internet'.[63] In contractual terms, acknowledgement of the threats from cyber attacks and the importance of cyber defence was understood in the ANZUS Treaty in 2011 under article V.[64] Here, cyber warfare was included in a suite of threats to Australia's 'territorial integrity, political independence . . . [and the] security of the partners' that will trigger activation of the ANZUS Treaty. This signalled an expansion of both threat designations and the understanding of the cyber battlespace domain, as well as a deepening of the joint alliance approach.[65]

Force and cognitive threat?

The shift in the ADF's view of cyberspace, to seeing it both as an enabler for generating and deploying military force and as a cognitive battlespace where defensive and offensive forces are deployed, arose from the adjustment of traditional forms of material connectivity among allies to non-linear changes in the war-fighting methods and offensive opportunities of the West's adversaries. These changes have resulted in unprecedented and continuing cyber attacks by state-based actors on liberal democratic institutions and values. While Australia's national intelligence and security agencies were constructing a defence force response in the emerging cyber-threat space, which is actively reorganizing institutional capacities and connecting into alliance resources, they are only in the early stages of fully comprehending the strategic vulnerabilities of liberal democracy to society-centric, cognitive warfare. According to Bracken, considerably more attention is assigned to operational matters than to strategic thinking, and the balance needs to be redressed.[66] Perhaps the cyber attacks on the political and government institutions of Australia reported in February 2019 will sound a wake-up call.

Driven by governance changes generated by intelligence reviews,[67] and party political efforts to accommodate conservative elements in the governing coalition parties, Australia has addressed the threat to national security posed by cognitive warfare through legislative and institutional reforms. It has done so because of 'unprecedented foreign intelligence activity against Australia',[68] emanating in particular from China. Legislative changes in June 2018 strengthened espio-

[63] Prime Minister and Cabinet, 'Australia's Cyber Security Strategy: enabling innovation, growth and prosperity', 2016, https://www.pmc.gov.au/sites/default/files/publications/australias-cyber-security-strategy.pdf.

[64] Clare Sullivan, 'Cybersecurity and the ANZUS Treaty: the issue of US–Australian retaliation', *Georgetown Journal of International Affairs*, 27 Aug. 2014, https://www.georgetownjournalofinternationalaffairs.org/online-edition/cybersecurity-and-the-anzus-treaty-the-issue-of-u-s-australian-retaliation.

[65] 'Australia–United States Ministerial Consultations (AUSMIN) 2011 joint communiqué', 15 Sept. 2011, https://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/1436994/upload_binary/1436994.pdf;fileType=application%2Fpdf#search=%22media/pressrel/1436994%22.

[66] Paul Bracken, 'Cyberwar and its strategic context', *Georgetown Journal of International Affairs* 18: 3, Fall 2017, pp. 147–57 at p. 148.

[67] Prime Minister and Cabinet, *2017 Independent Intelligence Review* (Canberra, June 2017), https://pmc.gov.au/sites/default/files/publications/2017-Independent-Intelligence-Review.pdf.

[68] Attorney-General for Australia, The Hon. Christian Porter MP, 'Australia's national security greatly enhanced with new laws', media release, 28 June 2018, https://www.attorneygeneral.gov.au/Media/Pages/Australias-national-security-greatly-enhanced-with-new-laws.aspx.

nage laws. Foreign interference was targeted with the Foreign Influence Transparency Scheme Act 2018, which aimed to make more visible the activities of foreign governments seeking to exercise influence in Australian political processes. The newly established Office of National Intelligence (ONI), located within the Department of Prime Minister and Cabinet, replaced and doubled in size the Office of National Assessments. The ONI is the new coordinating and integrating body for ten intelligence agencies, together comprising approximately 7,000 personnel with a combined budget of A$2 billion. In addition to legislative changes, in 2017 the Australian government established the 'super-ministry' of Home Affairs and placed under its aegis ASIO, the Australian Federal Police and the Border Force. The national security remit of Home Affairs is very broad, including counterterrorism, countering foreign interference and cyber security. The establishment in 2017 of a Critical Infrastructure Centre within Home Affairs signalled a move to more careful consideration of foreign investment in critical national assets. The unstated intention here was to monitor closely Chinese investment, especially by state-owned enterprises, and to give the foreign investment review board process more grounds to reject takeovers on national security grounds.

The cyber-enabled blurring of distinctions between foreign and domestic intelligence data collection, and the rapid processing of data for operationalization, resulted in the most substantive structural reform of Australia's national security architecture involving defence and intelligence since the 1980s. The institutional, technological and cultural challenge is how to maximize intended value-added gains from integrative effects with allies. Two powerful institutions, the ONI and Home Affairs, were created, though their capacity to work collaboratively was yet to be established fully in 2018. Nonetheless, pressing questions remain as to how Australia will redesign and redirect traditional military force to create strategic-level cognitive security in a hyperconnected world which facilitates society-centric warfare, and how it will do so beyond responses to infrastructure and espionage threats, and legislative reforms to limit foreign influence activities.

Two specific questions arise. First, Australia's 'last wars' were fought as part of the US-led alliance; can Australia's strategic culture and defence forces fight an adversary launching 'society-centric' warfare by increasing reliance on US cyber capabilities which are designed to secure the United States and US interests? Second, are networked cyber capabilities and their strategic rationale evolving sufficiently to defend against the 'weaponization' of social media in Australia? These are the challenges besetting Australia and its allies in the cyber and cognitive warfare space and, more broadly, liberal democracies across the globe. In August 2018 the Five Eyes group expressed concern about the effects of foreign interference on sovereign independence, values and interests.[69] Moves to share collective knowledge and coordinate responses, including with other democratic states in

[69] Department of Home Affairs, 'Five Country Ministerial 2018, official communiqué', 28–29 Aug. 2018, https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/five-country-ministerial-2018.

the event of a serious incident, are being made in the early stages of comprehending the problem. Lewis has argued that the United States and its allies have been hindered by the absence of a capability to instigate a cohesive and effective military response.[70] Exacerbating that hindrance is the accelerating speed with which adversaries are weaponizing information, and the speed and sophistication with which they are adapting their responses to defensive measures.[71]

Conclusion

Australia's approach to the use of force is shaped by a strategic culture and interests predicated on US military primacy to sustain order in the Pacific. Australia's involvement in wars as an expeditionary force in the early years of the present century remains illustrative of a sense of vulnerability born of the 'tyranny of distance'. Australia's experiences of war in the twentieth and twenty-first centuries foreshadowed profound battlespace transformations where the ground was increasingly difficult to defend, and adversaries were increasingly difficult to respond to offensively. The aim of a swift military victory in a kinetic conflict waged against a traditional state-based adversary dissipated in a new cyber-enabled battlespace which was ill-defined, highly contested and prolonged. What victory entailed and how one knew when it was achieved were increasingly problematic. Whereas the ADF fought adept tactical battles, adversaries operated increasingly with a different methodology and trajectory. Globally, Australia's geographic liminality is diminished not only by power transitions in the Indo-Pacific but also by the hyperconnectivity of global communications, which dismantles distinctions between the domestic and foreign.[72] The irony is that the absence of cyber liminality reinforces Australia's traditional sense of vulnerability.

What is understood only partially at the strategic level is the nature of cyber and cognitive interference by authoritarian states in the western liberal order. The goal is interference that exacerbates doubt and division along the fault-lines of domestic support for Australia's open, multicultural society, and for its liberal democratic political system and values. At this catalytic juncture of massive technological disruption, Australia faces challenges about, first, how to effectively enable defence in an increasingly unified threat environment; and, second, how to task a restructured intelligence community in conjunction with a military resourced for traditional, not cognitive and society-centric, warfare. Australia's vulnerabilities remain substantial, especially during the post-2016 transition phase for the new apparatuses of the national security architecture. Their strategic and imaginative challenges are to ensure national security at a time when the challenges of asymmetric socio-cognitive warfare, or the 'weaponization of information',

[70] Lewis, *Rethinking cybersecurity*, p. 36.

[71] Rand Waltzman, 'The weaponization of information: the need for cognitive security', CT-473, testimony presented before the Senate Armed Services Committee, Subcommittee on Cybersecurity, Rand Corporation, 27 April 2017, https://www.rand.org/pubs/testimonies/CT473.html.

[72] Michael Evans, *The tyranny of dissonance: Australia's strategic culture and way of war 1901–2005*, paper no. 306 (Land Warfare Studies Centre, Feb. 2005), p. 90.

are intensifying,[73] and before they are understood fully.[74] The question remains: what does a strategy for deployment of military force look like when technology recouples defence of the national interest with preservation of liberal democratic values? Complicating the challenge is that governance of the cyber and cognitive battlespace relies on access to US corporatized internet platforms which provide the technological medium through which defensive and offensive socio-political effects are realized. As attacks extend to liberal democratic governance, collaboration among allies must reach across government, the economy and the community in ways never previously attempted. Greater attempts at collaboration with the United States through formal alliance commitments, the Five Eyes agreement, and similar liberal democratic institutions and values seem likely; but they are unlikely to be made without difficulty.

[73] Philip Howard, Samuel Woolley and Ryan Calo, 'Algorithms, bots, and political communication in the US 2016 election: the challenge of automated political communication for election law and administration', *Journal of Information Technology and Politics* 15: 2, 2018, pp. 81–93.

[74] Gillian Bolsover and Philip Howard, 'Computational propaganda and big political data: moving toward a more critical research agenda', *Big Data* 5: 4, 2017, pp. 273–6.